TỈNH ỦY BẮC NINH
TIỂU BAN AN NINH MẠNG
*
Số 04 -QĐ/TBANM

ĐẢNG CỘNG SẢN VIỆT NAM

Bắc Ninh, ngày 22 tháng 4 năm 2026

QUYẾT ĐỊNH
ban hành Quy chế hoạt động của Đội Ứng cứu sự cố an ninh mạng tỉnh Bắc Ninh

---

Căn cứ Luật Tổ chức chính quyền địa phương ngày 16 tháng 6 năm 2025;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Quyết định số 03 -QĐ/TBANM ngày 22 tháng 4 năm 2026 của Trưởng Tiểu ban An ninh mạng tỉnh về việc thành lập Đội Ứng cứu sự cố an ninh mạng tỉnh Bắc Ninh;

Xét đề nghị của Công an tỉnh - Cơ quan Thường trực Tiểu ban An ninh mạng tỉnh Bắc Ninh,

TRƯỞNG TIỂU BAN AN NINH MẠNG
QUYẾT ĐỊNH

Điều 1. Ban hành kèm theo Quyết định này Quy chế hoạt động của Đội Ứng cứu sự cố an ninh mạng tỉnh Bắc Ninh.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Thủ trưởng, người đứng đầu các ban, cơ quan, đơn vị của Tỉnh ủy, UBND tỉnh; Giám đốc Công an tỉnh; các cơ quan, doanh nghiệp có liên quan và các thành viên Đội Ứng cứu sự cố an ninh mạng tỉnh Bắc Ninh chịu trách nhiệm thi hành Quyết định này.

Nơi nhận:
- Như Điều 3,
- Văn phòng BCĐ ANMQG (qua Cục A05, BCA) *(báo cáo)*,
- Thường trực Tỉnh ủy, HĐND, UBND tỉnh,
- Công an tỉnh, Bộ CHQS tỉnh,
- Đảng ủy, UBND các xã, phường,
- VNPT Bắc Ninh, Viettel Bắc Ninh, Mobifone Bắc Ninh, FPT Bắc Ninh,
- Lưu Văn phòng Tỉnh ủy, Công an tỉnh.

GIÁM ĐỐC CÔNG AN TỈNH
kiêm
PHÓ TRƯỞNG TIỂU BAN TT

ĐẢNG CỘNG SẢN VIỆT NAM
TỈNH ỦY BẮC NINH

Bùi Duy Hưng

QUY CHẾ
hoạt động của Đội Ứng cứu sự cố an ninh mạng tỉnh Bắc Ninh

(kèm theo Quyết định số 04-QĐ/TBANM ngày 22/4/2026 của Trưởng Tiểu ban An ninh mạng tỉnh Bắc Ninh)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Quy chế này quy định về nhiệm vụ, trách nhiệm, quyền hạn, nguyên tắc hoạt động và chế độ của Đội Ứng cứu sự cố an ninh mạng tỉnh Bắc Ninh *(viết tắt là Đội Ứng cứu sự cố).*

2. Quy chế này được áp dụng cho Đội Ứng cứu sự cố và các cơ quan, tổ chức, cá nhân có liên quan trong hoạt động điều phối, ứng cứu sự cố an ninh mạng trên địa bàn tỉnh.

Điều 2. Giải thích từ ngữ

1. Đội Ứng cứu sự cố là tổ chức/đơn vị do Tiểu ban An ninh mạng tỉnh thành lập nhằm triển khai các hoạt động, giải pháp sẵn sàng ứng phó hoặc ứng phó với các đe dọa, rủi ro; các lỗ hổng, điểm yếu; các sự cố đối với các hệ thống, cơ sở hạ tầng thông tin và không gian mạng trong phạm vi quản lý.

2. Vị trí chuyên trách về an toàn thông tin là vị trí đảm nhiệm nhóm công việc đặc trưng khác biệt, có cùng độ phức tạp, thuộc lĩnh vực an toàn thông tin (ATTT); thường sử dụng cùng nhóm kiến thức và kỹ năng. Khác với vị trí việc làm chuyên môn, cơ quan nào cũng có như: Quản lý nhân sự, tài chính,…

3. Sự cố an ninh mạng là sự kiện đã, đang xảy ra gây mất ATTT trên môi trường mạng (LAN, WAN, INTERNET) được phát hiện thông qua việc giám sát, đánh giá, phân tích của các cơ quan, tổ chức, cá nhân có liên quan hoặc được cảnh báo từ các chuyên gia, tổ chức về lĩnh vực an ninh mạng trong nước và trên thế giới.

4. Ứng cứu sự cố an ninh mạng là hoạt động nhằm xử lý, khắc phục sự cố gây mất an ninh mạng, gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, kiểm tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

Điều 3. Chức năng Đội Ứng cứu sự cố

Đội Ứng cứu sự cố có chức năng giám sát, kiểm tra, thực hiện các hoạt động ứng cứu sự cố an ninh mạng của các hệ thống thông tin trên địa bàn tỉnh *(trừ lĩnh vực quân sự, quốc phòng, cơ yếu);* cảnh báo kịp thời các vấn đề an toàn, an ninh thông tin; là đầu mối thực hiện hợp tác với các tổ chức an ninh mạng quốc gia, Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia.

Điều 4. Nhiệm vụ và quyền hạn của Đội Ứng cứu sự cố

1. Hỗ trợ các ban, cơ quan, đơn vị của Tỉnh ủy, UBND tỉnh; Đảng ủy, UBND các xã, phường và đơn vị liên quan về công tác đảm bảo an ninh mạng trong hoạt động ứng dụng công nghệ thông tin (CNTT) và tổ chức ứng cứu các sự cố an ninh mạng trên địa bàn tỉnh.

2. Là đầu mối của tỉnh, có nhiệm vụ liên kết, phối hợp với các đơn vị trong mạng lưới ứng cứu sự cố quốc gia *(dưới sự điều phối của Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia)* trong việc thu thập thông tin, kịp thời cảnh báo sự cố và các điểm yếu, lỗ hổng bảo mật, các nguồn tấn công mạng để các cơ quan, đơn vị chủ động phòng chống, giảm thiểu rủi ro.

3. Tham gia các khóa huấn luyện, diễn tập nâng cao năng lực và phát triển nhân lực Đội Ứng cứu sự cố.

4. Tham gia hoạt động ứng cứu khẩn cấp sự cố an ninh mạng quốc gia khi có yêu cầu từ Bộ Công an hoặc Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia do Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an chủ trì điều phối.

5. Tham gia các hoạt động của Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia; tham gia hoạt động phòng, chống chiến tranh thông tin, chiến tranh không gian mạng khi có yêu cầu của cơ quan chức năng.

6. Khi được sự đồng ý của lãnh đạo cơ quan, đơn vị chủ quản hệ thống thông tin bị sự cố, các thành viên Đội Ứng cứu sự cố có quyền truy cập vào hệ thống mạng, hệ thống ứng dụng CNTT, cơ sở dữ liệu, nhật ký hệ thống (log file) để phân tích, truy vết và thực hiện dưới sự giám sát của cơ quan, đơn vị bị sự cố.

Chương II
NGUYÊN TẮC, CHẾ ĐỘ LÀM VIỆC VÀ KINH PHÍ HOẠT ĐỘNG

Điều 5. Nguyên tắc hoạt động

1. Điều phối hoạt động ứng cứu sự cố an ninh mạng trong phạm vi của tỉnh.

2. Tổ chức ứng cứu sự cố an ninh mạng phải đúng quy trình ứng cứu sự cố, dựa trên tính chất, mức độ, phạm vi và nguyên nhân xảy ra sự cố; bảo đảm nhanh chóng, chính xác, kịp thời, hiệu quả và ATTT.

3. Thông tin được trao đổi, cung cấp trong quá trình điều phối, xử lý sự cố phải được bảo đảm bí mật theo yêu cầu của cơ quan, đơn vị gặp sự cố, trừ khi sự cố xảy ra có liên quan tới nhiều đối tượng khác cần phải cảnh báo hoặc phối hợp.

4. Việc trao đổi thông tin trong hoạt động điều phối phải được thực hiện bằng một hoặc nhiều hình thức như: Công văn, thư điện tử, điện thoại, FAX... Thành viên Đội Ứng cứu sự cố khi tiếp nhận thông tin phải chủ động xác thực đối tượng gửi nhằm bảo đảm tính chính xác của thông tin tiếp nhận.

Điều 6. Chế độ làm việc

1. Khi xảy ra sự cố phải ưu tiên cho hoạt động của Đội Ứng cứu sự cố, thực hiện nghiêm sự triệu tập, điều phối của Đội trưởng hoặc Đội phó khi được ủy quyền.

2. Thư ký, Thường trực Đội Ứng cứu sự cố giúp Đội trưởng và Đội phó trong hoạt động điều phối, ứng cứu sự cố.

3. Đội trưởng triệu tập thành viên Đội Ứng cứu sự cố, tổ chức phiên họp thường kỳ **06 tháng/lần** hoặc triệu tập họp đột xuất theo yêu cầu nhiệm vụ và yêu cầu của cơ quan cấp trên. Thời gian và địa điểm họp do Đội trưởng quyết định. Thư ký, Thường trực Đội Ứng cứu sự cố có trách nhiệm chuẩn bị các điều kiện cần thiết để tổ chức cuộc họp, tổng hợp biên bản họp và các nội dung khác theo yêu cầu của Đội trưởng.

4. Đội trưởng triệu tập và điều phối các thành viên khi có sự cố xảy ra; khi vắng mặt, ủy quyền cho Đội phó hoặc 01 thành viên thường trực là lãnh đạo thực hiện thẩm quyền của mình. Đội phó hoặc thành viên thường trực khi được ủy quyền được sử dụng thẩm quyền của Đội trưởng để điều phối các hoạt động và chịu trách nhiệm về các quyết định của mình trước Đội trưởng và trước pháp luật.

5. Thẩm quyền ký ban hành văn bản của Đội Ứng cứu sự cố:

a) Đội trưởng ký ban hành tất cả các văn bản của Đội Ứng cứu sự cố theo thẩm quyền;

b) Đội phó ký ban hành văn bản thực hiện văn bản điều phối sự cố từ cơ quan cấp trên *(Bộ Công an; Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia)*; các văn bản khác do Đội trưởng ủy quyền.

Điều 7: Chế độ thông tin, báo cáo

1. Trường hợp khi phát hiện sự cố khẩn cấp, Đội trưởng, Đội phó hoặc thành viên thường trực Đội Ứng cứu có thể thông báo bằng điện thoại, email công vụ để triệu tập thành viên, điều phối và thông báo bằng văn bản sau.

2. Báo cáo định kỳ **06 tháng (trước ngày 20/6), 01 năm (trước ngày 15/12)** theo quy định gửi Bộ Công an, Tiểu ban An ninh mạng tỉnh hoặc đột xuất khi có yêu cầu.

Điều 8. Kinh phí hoạt động

Đội Ứng cứu sự cố được đảm bảo kinh phí hoạt động từ nguồn ngân sách nhà nước theo các quy định của pháp luật.

Hằng năm, Công an tỉnh tổng hợp, xây dựng dự toán kinh phí, phối hợp với Sở Tài chính báo cáo Tỉnh ủy, UBND tỉnh xem xét, quyết định phân bổ kinh phí cho hoạt động của Đội Ứng cứu sự cố bổ sung vào dự toán chi ngân sách cho Tiểu ban An ninh mạng tỉnh đảm bảo theo quy định.

Chương III
HOẠT ĐỘNG ĐIỀU PHỐI, ỨNG CỨU SỰ CỐ

Điều 9. Tiếp nhận và xử lý thông báo, báo cáo sự cố

1. Các hình thức thông báo, báo cáo sự cố

a) Hình thức thông báo sự cố: Bằng công văn, thư điện tử, nhắn tin đa phương tiện hoặc thông qua hệ thống điều hành an ninh mạng quốc gia.

b) Hình thức báo cáo sự cố: Bằng văn bản giấy hoặc văn bản điện tử *(có ký tên, đóng dấu hoặc chữ ký số của người có thẩm quyền) (theo mẫu Phụ lục I)*.

2. Cơ quan, đơn vị, địa phương khi gặp sự cố không tự khắc phục được cần thông báo hoặc báo cáo sự cố tới thường trực Đội Ứng cứu sự cố hoặc thành viên Đội Ứng cứu sự cố *(theo mẫu Phụ lục I, II)*.

3. Khi phát hiện và nhận thấy sự cố nghiêm trọng, cơ quan, đơn vị phải có trách nhiệm thông báo ngay cho Thường trực Đội Ứng cứu sự cố.

4. Nội dung thông báo sự cố gồm: Tên, địa chỉ đơn vị, cá nhân thông báo sự cố; tên hoặc tên miền, địa chỉ IP của hệ thống thông tin bị sự cố; tên địa chỉ của đơn vị, cá nhân vận hành và cơ quan chủ quản hệ thống thông tin bị sự cố (nếu biết); mô tả sự cố và thời điểm phát hiện sự cố; kết quả xử lý sự cố đề xuất, kiến nghị và các thông tin liên quan khác (nếu có).

5. Thường trực Đội Ứng cứu sự cố tiếp nhận được thông báo sự cố phải báo cáo ngay cho Đội trưởng.

6. Đội trưởng quyết định điều phối các thành viên trong Đội; triệu tập cuộc họp (nếu cần); huy động các nguồn lực để xử lý sự cố khi cần thiết.

Điều 10. Quy trình ứng cứu sự cố an ninh mạng

1. Tiếp nhận, phân tích, ứng cứu ban đầu và thông báo sự cố.

a) Tiếp nhận, xác minh sự cố;

b) Triển khai các bước ưu tiên ứng cứu ban đầu;

c) Triển khai lựa chọn phương án ứng cứu;

d) Chỉ đạo xử lý sự cố (nếu cần);

đ) Báo cáo sự cố;

e) Điều phối công tác ứng cứu.

2. Triển khai ứng cứu, ngăn chặn và xử lý sự cố.

a) Triển khai thu thập chứng cứ, phân tích, xác định phạm vi, đối tượng bị ảnh hưởng;

b) Triển khai phân tích, xác định nguồn gốc tấn công, tổ chức ứng cứu và ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.

3. Xử lý sự cố, gỡ bỏ và khôi phục.

a) Xử lý sự cố, gỡ bỏ.

b) Khôi phục.

c) Kiểm tra, đánh giá hệ thống thông tin.

4. Tổng kết, đánh giá.

Điều 11. Ứng cứu sự cố

1. Đưa ra cảnh báo: Là đầu mối tiếp nhận cảnh báo của các cơ quan an ninh thông tin cấp trên. Xây dựng chương trình cảnh báo các lỗ hổng bảo mật đến các cơ quan, đơn vị.

2. Xử lý các lỗi và lỗ hổng bảo mật: Nghiên cứu, báo cáo các lỗ hổng cho các đơn vị ATTT cấp tỉnh; trực tiếp tiếp nhận và xử lý bảo mật từ đơn vị cấp trên. Trực tiếp, hướng dẫn các đơn vị xử lý các lỗ hổng bảo mật xảy ra trong hệ thống thông tin.

3. Kiểm tra, đánh giá, tư vấn bảo mật: Kiểm tra, đánh giá công tác đảm bảo an toàn, an ninh tại đơn vị, hỗ trợ các đơn vị xây dựng các chương trình bảo mật.

4. Xây dựng, phát triển công cụ bảo mật.

5. Phân tích rủi ro: Dựa trên công tác kiểm tra đánh giá an toàn tại các đơn vị đưa ra các cảnh báo về nguy cơ mất ATTT.

6. Điều tra sự cố: Kịp thời xử lý, phối hợp với các cơ quan chức năng điều tra các sự cố, cuộc tấn công vào hệ thống thông tin của các cơ quan, đơn vị.

Điều 12. Điều phối ứng cứu sự cố

1. Đội trưởng hoặc Đội phó thường trực thực hiện thông báo triệu tập, điều phối bằng văn bản đến các thành viên trong Đội Ứng cứu sự cố.

Thường trực Đội Ứng cứu sự cố thông báo cho các tổ chức, cá nhân gặp sự cố về yêu cầu phối hợp trong quá trình thực hiện điều phối và ứng cứu sự cố.

2. Thành viên Đội Ứng cứu sự cố tiếp nhận thông báo điều phối; phối hợp chặt chẽ với đơn vị xảy ra sự cố và các thành viên cùng tham gia ứng cứu tổ chức thực hiện hoạt động ứng cứu theo quy trình được quy định tại Điều 10 Quy chế này; báo cáo kết quả thực hiện cho Đội trưởng *(qua Thường trực Đội Ứng cứu sự cố)*.

3. Công tác ứng cứu kết thúc khi sự cố được khắc phục và hệ thống hoạt động trở lại bình thường.

4. Sau khi khắc phục sự cố phải thực hiện các công việc sau:

a) Rà soát, xác định nguyên nhân cơ bản gây ra sự cố.

b) Tổ chức kiểm tra lại và tham mưu giải pháp khắc phục triệt để sự cố.

c) Bảo đảm hệ thống hoạt động bình thường trước khi bàn giao hệ thống cho cơ quan, đơn vị chủ quản.

5. Cán bộ đảm nhận vai trò thư ký phải lưu trữ thông báo sự cố và biên bản xử lý sự cố; lưu trữ thông báo điều phối và báo cáo kết quả thực hiện khắc phục sự cố trong thời gian tối thiểu **01 năm.**

Điều 13. Đào tạo, hướng dẫn

Hằng năm, tổ chức xây dựng kế hoạch đào tạo, tập huấn ngắn hạn, trung hạn và dài hạn cho cán bộ phụ trách CNTT tại các cơ quan, đơn vị. Hướng dẫn công tác đảm bảo an ninh mạng cho các cán bộ chuyên trách CNTT trên địa bàn tỉnh Bắc Ninh.

Chương IV
TRÁCH NHIỆM VÀ QUYỀN HẠN CỦA TỔ CHỨC, CÁ NHÂN

Điều 14. Bộ phận Thường trực Đội Ứng cứu sự cố

1. Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh Bắc Ninh là đầu mối liên lạc, tiếp nhận thông tin điều phối ứng cứu sự cố an ninh mạng của tỉnh; các phản ánh sự cố, điều phối xử lý sự cố từ Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia; giúp Đội trưởng điều phối ứng cứu sự cố trên địa bàn tỉnh.

2. Thông tin liên hệ:

- Số điện thoại thường trực: Đồng chí Trần Viết Soái - Đội phó; điện thoại 0904.282359; đồng chí Vũ Anh Đức - Thành viên Thường trực, điện thoại 0982.072102.

- Email: ucscatttm@bacninh.gov.vn.

- Địa chỉ: Đường Hùng Vương, phường Tân Tiến, tỉnh Bắc Ninh.

Điều 15. Trách nhiệm và quyền hạn của Thường trực Đội Ứng cứu sự cố

1. Chủ trì, phối hợp với các thành viên tham mưu xây dựng và triển khai kế hoạch hoạt động của Đội; tổ chức hội thảo, hội nghị phổ biến, trao đổi thông tin, tập huấn, bồi dưỡng, đào tạo, huấn luyện, diễn tập về ứng cứu sự cố an ninh mạng; lập dự toán, quản lý và sử dụng kinh phí được cấp hằng năm cho hoạt động của Đội Ứng cứu sự cố theo các quy định hiện hành.

2. Thực hiện chức năng tham mưu, thực hiện điều phối các hoạt động ứng cứu sự cố trên toàn tỉnh và điều động các thành viên Đội Ứng cứu sự cố nhằm thực hiện hoặc phối hợp thực hiện việc ngăn chặn, xử lý, khắc phục sự cố an ninh mạng.

3. Tham mưu công tác thông tin, tuyên truyền về an ninh mạng và hoạt động ứng cứu sự cố. Tổng hợp, cập nhật, chia sẻ thông tin cảnh báo về các lỗ hổng, điểm yếu bảo mật, các nguy cơ sự cố và các biện pháp phòng ngừa, ngăn chặn, xử lý trên Cổng thông tin điện tử Công an tỉnh.

4. Đầu mối liên lạc ứng cứu sự cố trên địa bàn tỉnh và trong mạng lưới ứng cứu sự cố an ninh mạng trên toàn quốc; giúp Đội trưởng điều phối ứng cứu sự cố trên địa bàn tỉnh.

5. Theo dõi, cập nhật, thông báo kịp thời thông tin liên hệ của thành viên Đội Ứng cứu sự cố của tỉnh. Đề xuất, trình Cơ quan Thường trực của Tiểu ban An ninh mạng tỉnh ban hành quyết định kiện toàn thành viên khi có sự thay đổi nhân sự.

6. Thực hiện báo cáo định kỳ hoặc đột xuất khi có yêu cầu về hoạt động tiếp nhận và xử lý sự cố, gửi Tiểu ban An ninh mạng tỉnh, Bộ Công an và cơ quan cấp trên khác có thẩm quyền.

Điều 16. Trách nhiệm và quyền hạn của Đội trưởng

1. Chịu trách nhiệm trước Tiểu ban An ninh mạng về toàn bộ hoạt động của Đội Ứng cứu sự cố; chủ trì các cuộc họp, điều phối, quyết định tổ chức ứng cứu; triệu tập các thành viên để xử lý và khắc phục sự cố an ninh mạng.

2. Chủ trì tổ chức ứng cứu sự cố an ninh mạng trên địa bàn tỉnh, điều phối, phân công các thành viên trong Đội Ứng cứu sự cố tham gia ứng cứu khi có sự cố xảy ra. Là đầu mối liên hệ, phối hợp với Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia, các doanh nghiệp cung cấp dịch vụ Internet và các đơn vị liên quan.

3. Quyết định hình thức điều phối các hoạt động ứng cứu sự cố và chịu trách nhiệm về các yêu cầu điều phối.

Điều 17. Trách nhiệm và quyền hạn của Đội phó

1. Giúp Đội trưởng điều hành các hoạt động của Đội Ứng cứu sự cố, chịu trách nhiệm trước Đội trưởng về nhiệm vụ được giao; đề xuất kế hoạch, biện pháp kỹ thuật tăng cường công tác đảm bảo an ninh mạng.

2. Chỉ đạo các thành viên trong các hoạt động phòng ngừa, ngăn chặn và xử lý sự cố mạng máy tính theo thẩm quyền và nhiệm vụ được phân công; thay mặt Đội trưởng điều hành các hoạt động của Đội Ứng cứu sự cố khi được ủy quyền.

3. Thực hiện các nhiệm vụ do Đội trưởng phân công và tham gia xây dựng kế hoạch hoạt động hằng năm của Đội.

Điều 18. Trách nhiệm và quyền hạn của các thành viên Đội Ứng cứu sự cố

1. Tham mưu cho Thủ trưởng cơ quan, đơn vị xây dựng và triển khai thực hiện Kế hoạch, phương án ứng phó sự cố bảo đảm an ninh mạng; chịu trách nhiệm thường trực công tác ứng cứu sự cố tại cơ quan, đơn vị công tác.

2. Thường xuyên theo dõi các cảnh báo trên nền tảng điều phối xử lý sự cố an ninh mạng của tỉnh được giao quản lý, kịp thời phát hiện các dấu hiệu bất thường, phản ánh, thông tin về sự cố được quy định tại khoản 4 Điều 9 Quy chế này, báo cáo kịp thời cho Đội trưởng để thực hiện công tác điều phối ứng cứu sự cố.

3. Tiếp nhận và xử lý các thông báo sự cố hoặc văn bản triệu tập xử lý sự cố từ Đội trưởng, Đội phó và Thường trực Đội Ứng cứu sự cố. Phối hợp, hỗ trợ các thành viên khác trong Đội Ứng cứu sự cố, cán bộ phụ trách CNTT của các cơ quan, đơn vị trong việc áp dụng các biện pháp, giải pháp kỹ thuật nhằm bảo đảm an ninh mạng cho các hệ thống thông tin.

4. Kịp thời báo cáo, đề xuất giải quyết những khó khăn, vướng mắc trong quá trình thực hiện nhiệm vụ cho Đội trưởng hoặc Đội phó để kịp thời có sự chỉ đạo, xử lý.

5. Tham gia đầy đủ các cuộc họp định kỳ, đột xuất và hoạt động ứng cứu sự cố khi được triệu tập. Tham gia góp ý, đề xuất xây dựng Kế hoạch hoạt động hằng năm của Đội Ứng cứu sự cố; có quyền được chia sẻ thông tin, kinh nghiệm, tham gia các hoạt động diễn tập ứng cứu sự cố, các khóa đào tạo, bồi dưỡng về an ninh mạng và ứng cứu sự cố do Công an tỉnh triệu tập.

6. Định kỳ (06 tháng, 01 năm) báo cáo tổng hợp về hoạt động tiếp nhận và xử lý sự cố *(theo mẫu Phụ lục III)*.

Điều 19. Trách nhiệm của cơ quan quản lý thành viên của Đội Ứng cứu sự cố

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tạo điều kiện và ưu tiên cho thành viên Đội Ứng cứu sự cố thuộc đơn vị mình quản lý thực hiện các hoạt động của Đội Ứng cứu sự cố khi được triệu tập, điều phối.

2. Kịp thời thông báo về Công an tỉnh cập nhật danh sách thành viên tham gia Đội Ứng cứu sự cố khi có thay đổi.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 20. Tổ chức thực hiện

1. Công an tỉnh chủ trì tổ chức, kiểm tra, hướng dẫn Đội Ứng cứu và các cơ quan, đơn vị có liên quan thực hiện Quy chế này; kịp thời phát hiện và phối hợp với cơ quan chức năng tham mưu xử lý những trường hợp vi phạm.

2. Căn cứ kết quả hoạt động của mỗi thành viên, Đội Ứng cứu sự cố xem xét, đề nghị cấp có thẩm quyền khen thưởng theo quy định.

3. Trong quá trình thực hiện quy chế, nếu có vướng mắc, phát sinh, đề nghị các cơ quan, đơn vị, cá nhân phản ánh với Tiểu ban An ninh mạng tỉnh (qua Công an tỉnh) để xem xét, quyết định.

Phụ lục I
MẪU BÁO CÁO BAN ĐẦU SỰ CỐ MẠNG
(kèm theo Quyết định số 04-QĐ/TBANM ngày 22/4/2026 của Trưởng Tiểu ban An ninh mạng tỉnh Bắc Ninh)

BÁO CÁO BAN ĐẦU SỰ CỐ MẠNG

Tên tổ chức/cá nhân báo cáo sự cố (*).....

Địa chỉ: (*) .....

Điện thoại (*) .....

Email (*).....

NGƯỜI LIÊN HỆ

Họ và tên (*)..... Chức vụ: .....

Điện thoại (*).....Email (*).....

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*
Cơ quan chủ quản:	*Điền tên cơ quan chủ quản*
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố và tên miền, địa chỉ IP liên quan*
Phân loại cấp độ của hệ thống thông tin (nếu có)	□ Cấp độ 1 □ Cấp độ 2 □ Cấp độ 3 □ Cấp độ 4 □ Cấp độ 5
Tổ chức cung cấp dịch vụ an toàn thông tin (nếu có):	*Điền tên nhà cung cấp ở đây*
Tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)	*Điền tên nhà cung cấp ở đây*
Dải địa chỉ Public IP kết nối với hệ thống bên ngoài:	*Điền thông tin ở đây*
Mô tả sơ bộ sự cố (*)	
Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Cũng vui lòng xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố: …… …… …… ……	

Ngày phát hiện sự cố (*): / / (dd/mm/yyyy)	Thời gian phát hiện (*):	..... giờ.... phút

HIỆN TRẠNG SỰ CỐ (*)

□ Đã được xử lý □ Chưa được xử lý

CÁCH THỨC PHÁT HIỆN **(Đánh dấu những cách thức được sử dụng để phát hiện sự cố)*

□ Qua hệ thống phát hiện xâm nhập □ Kiểm tra dữ liệu lưu lại (Log File)

□ Nhận được thông báo từ:..... .. ..

□ Khác, đó là:..... .. ..

ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO *

□ Thành viên mạng lưới chịu trách nhiệm ứng cứu sự cố cho tổ chức, cá nhân

□ ISP đang trực tiếp cung cấp dịch vụ

□ Cơ quan điều phối

THÔNG TIN BỔ SUNG VỀ HỆ THỐNG XẢY RA SỰ CỐ

■ Hệ điều hành .....Version..... . .

■ Các dịch vụ có trên hệ thống *(Đánh dấu những dịch vụ được sử dụng trên hệ thống)*

□ Web server □ Mail server □ Database server

□ Dịch vụ khác, đó là..... .. .. ……

• Các biện pháp an toàn thông tin đã triển khai *(Đánh dấu những biện pháp đã triển khai)*

□ Antivirus □ Firewall □ Hệ thống phát hiện xâm nhập

□ Khác:

■ Các địa chỉ IP của hệ thống *(Liệt kê địa chỉ IP sử dụng trên Internet, không liệt kê địa chỉ IP nội bộ)*……..

■ Các tên miền của hệ thống……..

■ Mục đích chính sử dụng hệ thống……...

…….

■ Thông tin gửi kèm

□ Nhật ký hệ thống □ Mẫu virus/mã độc □ Khác:

■ Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật:

□ Có □ Không

KIẾN NGHỊ, ĐỀ XUẤT HỖ TRỢ

Mô tả về đề xuất, kiến nghị
Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ ứng cứu (nếu có)
……
……

…… …… ……

THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ*:…/…/…/…/… (ngày/tháng/năm/giờ/phút)

CÁ NHÂN/NGƯỜI ĐẠI DIỆN
THEO PHÁP LUẬT
(Ký tên, đóng dấu)

Chú thích:
1. Phần (*) là những thông tin bắt buộc. Các phần khác có thể loại bỏ nếu không có thông tin.
2. Sử dụng tiêu đề (subject) bắt đầu bằng "[TBSC]" khi gửi thông báo qua email.

Phụ lục II

MẪU BÁO CÁO KẾT THÚC ỨNG PHÓ SỰ CỐ

(kèm theo Quyết định số 04-QĐ/TBANM ngày 22/4/2026 của Trưởng Tiểu ban An ninh mạng tỉnh Bắc Ninh)

BÁO CÁO KẾT THÚC ỨNG PHÓ SỰ CỐ

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO

- Tên tổ chức/cá nhân báo cáo sự cố (*)
- Địa chỉ: (*) ..... ……
- Điện thoại (*).....
- Email (*)…… ..... ……

KÝ HIỆU BÁO CÁO BAN ĐẦU SỰ CỐ: Số ký hiệu …..Ngày báo cáo: / /202..

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*
Cơ quan chủ quản:	*Điền tên cơ quan chủ quản*
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố*
Phân loại cấp độ của hệ thống thông tin, (nếu có)	□ Cấp độ 1 □ Cấp độ 2 □ Cấp độ 3 □ Cấp độ 4 □ Cấp độ 5

Tên/Mô tả về sự cố

Ngày phát hiện sự cố (*)…/…/… (dd/mm/yyyy)	Thời gian phát hiện (*):	….giờ.... phút

Kết quả xử lý sự cố
Cung cấp, tóm tắt tổng quát về những gì đã xảy ra và cách thức giải quyết, đề xuất giải pháp ứng cứu sự cố nhằm xử lý nhanh sự cố, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự trong tương lai

…… …… …… ……

Các tài liệu đính kèm
Liệt kê các tài liệu liên quan (báo cáo diễn tập sự cố; phương án xử lý, log file…)

CÁ NHÂN/ NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT
(Ký tên, đóng dấu)

Chú thích: Phần (*) là những thông tin bắt buộc. Các phần khác có thể loại bỏ nếu không có thông tin.

Phụ lục III
MẪU BÁO CÁO ĐỊNH KỲ
(kèm theo Quyết định số 04-QĐ/TBANM ngày 22/4/2026 của Trưởng Tiểu ban An ninh mạng tỉnh Bắc Ninh)

Kính gửi: .....

BÁO CÁO TỔNG HỢP (06 THÁNG, 01 NĂM) VỀ HOẠT ĐỘNG TIẾP NHẬN VÀ XỬ LÝ SỰ CỐ

□ Từ tháng ...../20 ... đến tháng ..../20...

Tên cơ quan/tổ chức:..... .. ..

Địa chỉ: ....

1. Số lượng sự cố và cách thức xử lý

Loại sự cố/tấn công mạng	Số lượng	Số sự cố tự xử lý	Số sự cố có sự hỗ trợ xử lý từ các tổ chức khác	Số sự cố có hỗ trợ xử lý từ tổ chức nước ngoài	Số sự cố đề nghị VNCERT hỗ trợ xử lý	Thiệt hại ước tính
Từ chối dịch vụ						
Tấn công giả mạo						
Tấn công sử dụng mã độc						
Truy cập trái phép, chiếm quyền điều khiển						
Thay đổi giao diện						
Mã hóa phần mềm, dữ liệu, thiết bị						
Phá hoại thông tin, dữ liệu, phần mềm						
Nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu						
Tấn công tổng hợp sử dụng kết hợp nhiều hình thức						
Các hình thức tấn công khác						
Tổng số:						

2. Danh sách các tổ chức hỗ trợ xử lý sự cố

.....

3. Danh sách các tổ chức nước ngoài hỗ trợ xử lý sự cố

.....

4. Đề xuất kiến nghị.....

..... ngày .... tháng .... năm .....

NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT

(Ký tên, đóng dấu)